PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-028405
(43)Date of publication of application : 31.01.1995

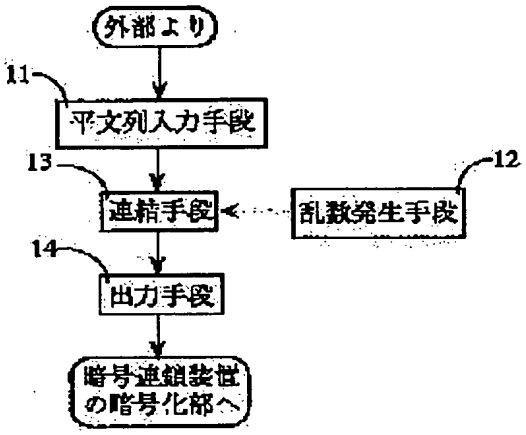
(51)Int.Cl. G09C 1/06
H04L 9/06
H04L 9/14

(21)Application number : 05-174527
(22)Date of filing : 14.07.1993

(71)Applicant : NEC CORP
(72)Inventor : MIYANO HIROSHI
MIYAUCHI HIROSHI

(54) CIPHERING PREPROCESSOR AND DECIPHERING POSTPROCESSOR FOR CIPHER CHAIN

(57)Abstract:
PURPOSE: To provide a cipher chaining device which can make use of the advantages of a cipher chaining system and a deciphering device for deciphering a cipher text by the cipher chaining device even when a plaintext is only one block long like it is used for certification by eliminating the weakness that starting one block has in a cipher chaining system and increasing the difficulty of deciphering.
CONSTITUTION: The ciphering preprocessor which preprocesses the input of the cipher chaining device is provided with a means 11 which inputs an array of plaintexts to be ciphered, a random number generating means 12 which generates a random number array with predetermined bit length, a coupling means 13 which couples the random bit array generated by the random number generating means 12 with the head of the array of plaintexts, and an output means 14 which sends and receives the array consisting of the coupled random numbers and plaintexts to and from the cipher chaining device.



LEGAL STATUS

[Date of request for examination]	14.07.1993
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2541113
[Date of registration]	25.07.1996
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平7－28405

(43)公開日　平成７年(1995)１月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ	1/06		8837－5L		
Ｈ０４Ｌ	9/06				
	9/14				
				Ｈ０４Ｌ　9/ 02	Ｚ

審査請求　有　　請求項の数２　ＯＬ　（全　４　頁）

(21)出願番号　特願平5－174527

(22)出願日　平成５年(1993)７月14日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　宮野　浩
東京都港区芝五丁目７番１号　日本電気株式会社内

(72)発明者　宮内　宏
東京都港区芝五丁目７番１号　日本電気株式会社内

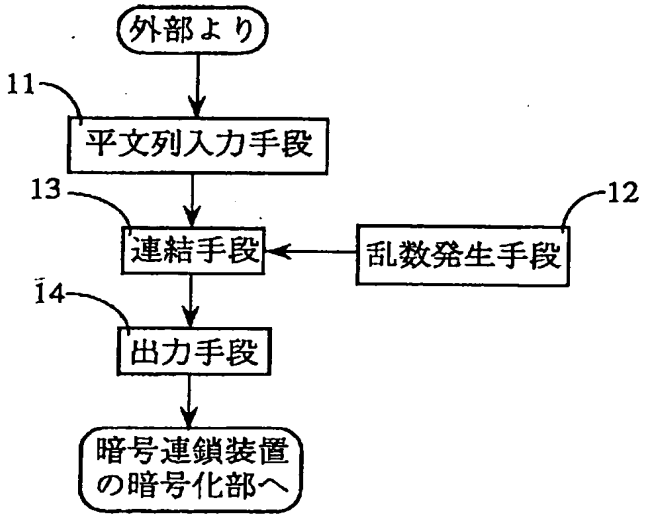
(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　暗号連鎖における暗号化前処理装置および復号後処理装置

(57)【要約】

【目的】　暗号連鎖方式において、最初の１ブロックが持つ弱さを解消し、解読の困難さを増大させるとともに、認証に用いる場合のように平文の長さが１ブロックしかないような場合にも暗号連鎖方式の利点を生かせるような暗号連鎖装置および該暗号連鎖装置によって暗号化された暗号文を復号するための復号装置を提供すること。

【構成】　暗号連鎖装置の入力を前処理を行う暗号化前処理装置において、暗号化されるべき平文の列を入力する手段１１と、予め定められたビット長の乱数列を発生する乱数発生手段１２と、該乱数発生手段によって発生されたランダムなビット列を該平文の列の先頭に結合する連結手段１３と、上記結合された乱数と平文からなる列を暗号連鎖装置に受け渡すための出力手段１４を有することを特徴とする。



1

【特許請求の範囲】

【請求項１】　平文の列を一定数のビット毎に区切った平文ブロックを逐次入力とし暗号鍵の制御を受けかつ該ブロックに先行するブロックの処理内容に依存した処理により該平文ブロックに対応する暗号ブロックを生成し逐次生成された暗号文ブロックを結合して該平文の列に対する暗号文の列を生成する暗号連鎖装置の入力の前処理を行う暗号化前処理装置において、暗号化されるべき平文の列を入力する手段と、予め定められたビット長からなる常には同じ値になることのないビット列を発生する乱数発生手段と、前記乱数発生手段によって発生されたランダムなビット列を前記平文の列の先頭に結合する連結手段と、前記ランダムなビット列と平文の列との結合を暗号連鎖装置に受け渡すための出力手段を有することを特徴とする暗号連鎖における暗号化前処理装置。

【請求項２】　暗号文を復号する復号装置の出力に対して後処理を施した平文を出力する復号後処理装置において、暗号連鎖装置から復号された平文列を受け取るための入力手段と、予め定められた長さのビット列を前記平文列の先頭から取り除く冗長ビット除去手段と、前記冗長ビット除去手段によって加工された平文列を最終的な平文として出力する平文列出力手段を有することを特徴とする暗号連鎖における復号後処理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、暗号化および復号装置に関するものである。

【０００２】

【従来の技術】ＤＥＳのＣＢＤモード（昭４８－１７２３４暗号方法、たとえば「現代暗号理論」池野信一、小山謙二著、社団法人電子情報通信学会１９８６年のｐ．６６に解説）に代表される従来の暗号連鎖方式は、一つの平文ブロツクを暗号化する度にその結果あるいは経過に基づく情報を暗号器に回帰させその情報が次回およびそれ以降のブロックに対する暗号化に影響を及ぼすようにした暗号化方式である。この方式の特徴は、平文が持つ統計的な特徴を攪乱する効果に加えて、過去の暗号化処理の履歴が暗号化関数に影響を及ぼすために解読の企てに対して強いことなどが挙げられる。

【０００３】暗号系の用途は様々であり、通信文やファイルなどの暗号化だけではなく、計算器の利用に係るユーザやプロセスなどの認証のために用いられたりユーザのパスワードを格納しておくために用いられたりすることもある。これらの用途によっては、暗号化すべき平文の長さが１ブロック分しかなく、したがって暗号連鎖がおこらない内に暗号化が終了してしまうこともありうる。また、そうでなくても一般に暗号連鎖方式は最初の１ブロックだけは連鎖の効果をうけていないので、これが解読の端緒となるおそれがある。これを防ぐためには、回帰された情報を記憶する記憶部の初期値を暗号化

2

側と復号側で共有する方法も考えられるが、それは双方で共有する秘密情報の増大を招き、鍵を管理する負担を増大させる効果となる。

【０００４】

【発明が解決しようとする課題】本発明の目的は、暗号連鎖方式において、最初の１ブロックが持つ弱さを解消し、解読の困難さを増大させるとともに、認証に用いる場合のように平文の長さが１ブロックしかないような場合にも暗号連鎖方式の利点を生かせるような暗号連鎖装置および該暗号連鎖装置によって暗号化された暗号文を復号するための復号装置を提供することである。

【０００５】

【課題を解決するための手段】第１の発明の暗号化前処理装置は、平文の列を一定数のビット毎に区切った平文ブロックを逐次入力とし暗号鍵の制御を受けかつ該ブロックに先行するブロックの処理内容に依存した処理により該平文ブロックに対応する暗号ブロックを生成し逐次生成された暗号文ブロックを結合して該平文の列に対する暗号文の列を生成する暗号連鎖装置の入力の前処理を行う暗号化前処理装置において、暗号化されるべき平文の列を入力する手段と、予め定められたビット長からなる常には同じ値になることのないビット列を発生する乱数発生手段と、前記乱数発生手段によって発生されたランダムなビット列を前記平文の列の先頭に結合する連結手段と、前記ランダムなビット列と平文の列との結合を暗号連鎖装置に受け渡すための出力手段を有することを特徴とする。

【０００６】第２の発明の復号後処理装置は、暗号文を復号する復号措置の出力に対して後処理を施して平文を出力する復号後処理装置において、暗号連鎖装置から復号された平文列を受け取るための入力手段と、予め定められた長さのビット列を前記平文列の先頭から取り除く冗長ビット除去手段と、前記冗長ビット除去手段によって加工された平文列を最終的な平文として出力する平文列出力手段を有することを特徴とする。

【０００７】

【作用】本発明における暗号化の前処理および後処理について述べる。

【０００８】一般に、暗号連鎖方式においては、ある平文ブロックを暗号化する際には、それ以前に処理された平文に依存した暗号化処理が行われ、それによって複雑な暗号化関数を実現し解読を困難にしている。しかし、第１の平文ブロックを暗号化する際には、該平文ブロックに先行する平文ブロックが存在しないので連鎖による効果が全く得られない。したがって、ある暗号連鎖方式を何度も使用すると、それぞれの第１ブロックは全く同じ暗号化関数で処理されることになり、その結果暗号を解読しようとする者に解読の手がかりを与えてしまう可能性がある。

【０００９】本発明の原理は平文列の先頭にランダムに

生成されたビットの列を付加することにある。このランダムなビット列は暗号化を行う装置と同じ装置内で暗号化処理の直前に生成することが可能なので通常の平文と比較してその内容が第三者に漏れる可能性が著しく小さい。平文が漏れる可能性が小さいと言うことは既知平文攻撃を喫するおそれが小さいということである。

【００１０】また、平文の先頭に付加するランダムなビット列はその内容を予め受信者と打ち合わせておく必要がなく、付加するビットの長さだけを打ち合わせておけば十分であり、しかもその長さは秘密にしておく必要もない。したがって、暗号連鎖装置内のあるパラメータの初期値を予め示し合わせておく方法に比べて送信者及び受信者が管理しなければならない秘密情報が増えることはない。

【００１１】

【実施例】図１に第１の発明の暗号化前処理装置の実施例を、図２に図１に示した実施例で用いる乱数発生手段の構成例を、図３に第２の発明の復号後処理装置の実施例を示した。

【００１２】図１において暗号化前処理装置は、平文列入力手段１１、乱数発生手段１２、連結手段１３および出力手段１４とからなる。平文の列が平文入力手段１１から入力されると、乱数発生手段１２で予め定められた長さのランダムなビット列を発生する。該ビット列を冗長ビットと呼ぶ。次に、連結手段１３において、冗長ビットが先頭になるように冗長ビットと上記平文列を連結し、出力装置１４はその結果得られたビット列を暗号連鎖装置の入力として暗号連鎖装置に受け渡す。

【００１３】図２に第１の発明で用いる乱数発生手段１２の一例を示す。この例では、計算機内部のタイムスタンプを暗号鍵としてＤＥＳによって初期定数を暗号化し、暗号文を回帰させて繰り返し暗号化を行う。この際、各暗号文の先頭の１ビットを乱数列の一部として連結手段１３に受け渡す。ＤＥＳによる暗号化を連結手段１３で必要とする乱数列のビットの回数だけ行うことにより、乱数発生手段１２としての機能が実現される。

【００１４】図３において復号後処理装置は、入力手段３１、冗長ビット除去手段３２および平文列出力手段３３とからなる。入力手段３１は、暗号連鎖装置の復号装置から復号処理の済んだビット列を受け取り冗長ビット除去手段３２に受け渡す。冗長ビット除去手段３２は、受け取ったビット列の先頭から予め定められた数のビット列を除去し平文列出力手段３３に受け渡す。平文列出力手段３３は受け取ったビット列を外部に出力される。

【００１５】上記実施例における各ビット列の構造の例*

*を図４に示す。図４の例では、図の見やすさのために平文はブロックに区切られているが、実際には本発明の装置内ではこのように区切られている必要は必ずしもない。乱数発生手段１２で生成する冗長ビットの予め定められた長さはこの例ではブロック長よりも長くなっている。もとの平文列（ｐ１，ｐ２，．．．）は、上記実施例において平文列入力手段１１が外部より受け取る平文列および平文列出力手段３３が外部に出力する平文列であり、乱数発生装置で生成した冗長ビットは乱数発生手段１２によって生成され冗長ブロック除去手段３２によって除去されるビット列であり、暗号連鎖装置用の平文（ｒ１，ｒ２，ｐ１，ｐ２，．．．）は図１の出力手段１４から暗号連鎖装置の暗号化部に手渡され、かつ暗号連鎖装置の復号部から図３の入力手段３１に手渡されるビット列である。

【００１６】

【発明の効果】本発明では、予め定められた長さのランダムなビット列を冗長な情報として平文の先頭に付加し、この冗長なビット列は他とは全く独立に生成しうるので暗号が解読されてしまった場合意外には他に洩れる虞はない。したがって、選択平文攻撃は既知平文攻撃を行い得る解読者に対してもこのビット列は未知の情報となり、解読を困難にする。暗号文の正当な受信者にとって、復号の際にこの冗長ビットをあらかじめ知っている必要はなく、共有すべき秘密情報が増大することもない。

【図面の簡単な説明】

【図１】第１の発明の暗号化前処理装置の一実施例を示すブロック図。

【図２】第１の発明における乱数発生手段の一構成例を示すブロック図。

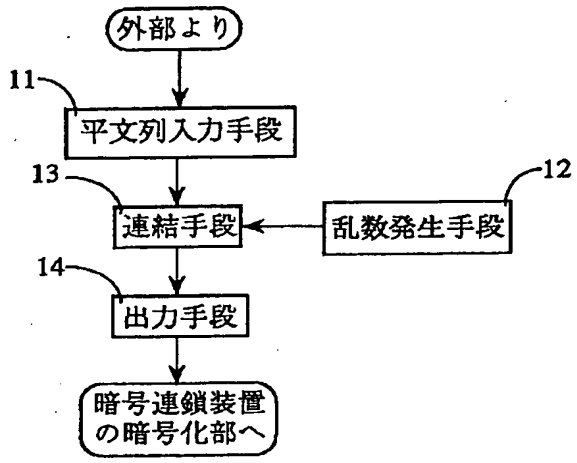
【図３】第２の発明の復号後処理装置の一実施例を示すブロック図。

【図４】本発明において取り扱われるビット列の構造の一例を示す図。

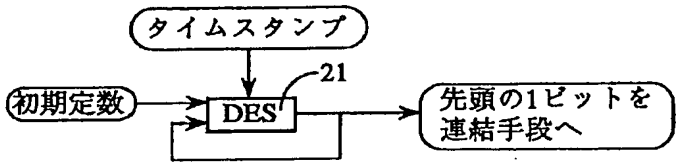
【符号の説明】

１１　平文列入力手段
１２　乱数発生手段
１３　連結手段
１４　出力手段
２１　暗号化装置ＤＥＳ
３１　入力手段
３２　ブロック除去手段
３３　平文列出力手段

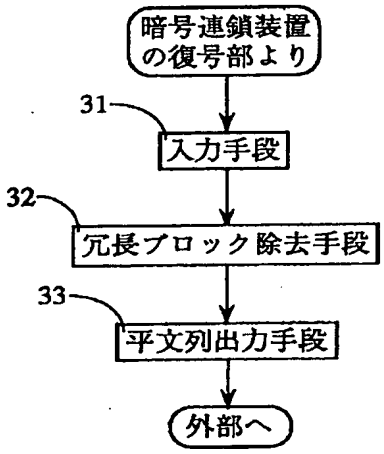
【図１】


外部より
11
平文列入力手段
13
連結手段
12
乱数発生手段
14
出力手段
暗号連鎖装置
の暗号化部へ

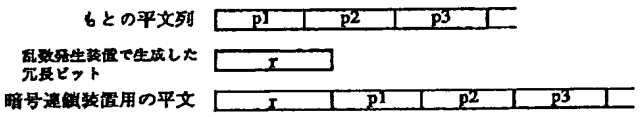
【図２】


タイムスタンプ
21
初期定数
DES
先頭の1ビットを
連結手段へ

【図３】


暗号連鎖装置
の復号部より
31
入力手段
32
冗長ブロック除去手段
33
平文列出力手段
外部へ

【図４】


もとの平文列
p1
p2
p3
乱数発生装置で生成した
冗長ビット
r
暗号連鎖装置用の平文
r
p1
p2
p3